Amendments to the Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Currently Amended) A method of securely transmitting a message to a receiving device, comprising the steps of:

(a) encrypting a first part of ~~said~~ the message with a first level of encryption to produce a first message portion;

(b) processing a second part of ~~said~~ the message with a second level of encryption to produce a second message portion, including selecting ~~with~~ the second level of encryption ~~selected~~ from [[the]] a group consisting of: (i) no encryption, and (ii) a level of encryption less strong than ~~said~~ the first level of encryption;

(c) transmitting ~~said~~ the first message portion and the second message ~~portions~~ portion over at least one transmission channel; and

[[(e)]] (d) providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message.

2. (Currently Amended) The method of ~~claim1~~ claim 1, ~~including the further step of~~ further comprising:

determining whether at least part of said first message portion should be decrypted upon receipt, and if so decrypting at least part of said first message portion to produce data from said first part of said message.

3. (Currently Amended) The method of claim 2, ~~including the further step of~~ further comprising:

determining whether at least part of said second message portion should be decrypted upon receipt, and if so decrypting at least part of said second message portion to produce data from said second part of said message.

4.   (Currently Amended) The method of claim 1, wherein in step (a) said first part of said message is encrypted with an asymmetric algorithm and said first message portion is decrypted on receipt and provided to the receiving device.

5.   (Currently Amended) The method of claim 1, wherein said first part of said message is encrypted for transmission, said second part of said message is not encrypted for transmission, and neither of said first and second message portions are decrypted upon receipt.

6.   (Currently Amended) The method of claim 1, wherein said first part of said message is encrypted for transmission, said second part of said message is encrypted for transmission with said second level of encryption less strong than said first level of encryption, and said second message portion is decrypted upon receipt.

7.   (Currently Amended) The method of claim 6, wherein said first message portion is decrypted upon receipt.

8.   (Currently Amended) The method of claim 1, wherein said first part of said message is encrypted for transmission, said second part of said message is not encrypted for transmission, and part of said first message portion is decrypted upon receipt.

9.   (Currently Amended) The method of claim 1, wherein said first part of said message is encrypted for transmission with said first level of encryption, said second part of said message is encrypted for transmission with said second level of encryption less strong than said first level, and part of said first message portion is decrypted upon receipt and provided to the receiving device.

10.   (Currently Amended) The method of claim 9, wherein said second message portion is decrypted upon receipt and provided to the receiving device.

Atty. Dkt. No. 1875.3820001

11.   (Currently Amended)   The method of claim 1, wherein said first message portion and said second message portion are divided into frames and in step (c) frames of said first message portion and frames of said second message portion are alternately transmitted over said at least one transmission channel.

12.   (Currently Amended)   The method of claim 1, wherein said message comprises speech data and said transmission channel comprises a mobile telephone system channel.

13.   (Currently Amended)   The method of claim 12, wherein a fraction of the speech data sufficient to prevent understanding of an intercepted message is strongly encrypted and transmitted in said first message portion.

14.   (Currently Amended)   The method of claim 12, wherein said message includes video telephone data and said video telephone data is at least partially encrypted and is not decrypted upon receipt unless one or more subscribers involved in exchanging the message has agreed to pay for video telephone service.

15.   (Currently Amended)   The method of claim 12, ~~including the further steps of~~ further comprising:

        encoding said speech data to produce a coded data set;

        in step (a), encrypting and transmitting in said first message portion encoding data useful in decoding said coded data set;

        in step (b), selecting and applying said second level of encryption to said coded data set to form said second message portion;

        decrypting said encoding data upon receipt; and

        using said encoding data to decode said coded data set to obtain said speech data.

16.   (Currently Amended)   The method of claim 14, wherein said encoding step is performed with a speech codec.

Atty. Dkt. No. 1875.3820001

17.   (Currently Amended) The method of claim 1, wherein said transmitting step includes the step of transmitting information indicating which portions of the transmission are encrypted.

18.   (Currently Amended) The method of claim 17, wherein said first message portion and said second message portion are comprised of a plurality of frames.

19.   (Currently Amended) The method of claim 18, wherein encrypted frames comprise data indicating a level of encryption applied to said encrypted frames.

20.   (Currently Amended) The method of claim 19, wherein said level indicating data is a frame encryption flag.

21.   (Currently Amended) The method of claim 1, wherein said message comprises video data and said transmission channel comprises a video distribution channel.

22.   (Currently Amended) The method of claim 21, wherein said video distribution channel comprises a cable television distribution channel.

23.   (Currently Amended) The method of claim 21, including the further steps of further comprising:

selecting a plurality of key data elements of said video data containing information needed to properly process and display the video data;

in step (a), encrypting and transmitting in said first message portion said key data elements;

in step (b), selecting and applying said second level of encryption to at least some of said video data not designated as key data elements;

decrypting said key data elements upon receipt; and

using data from said key data elements to process and display said video data.

Atty. Dkt. No. 1875.3820001

24.   (Currently Amended) The method of claim 23, wherein said key data elements contain I-signal video information.

25. - 30. (Cancelled)

31.   (Currently Amended) A method of securely transmitting a message to a receiving device, comprising the steps of:

(a)   selecting a first encryption algorithm;

(b)   encrypting a first part of said message with said first encryption algorithm to produce a first data set;

(c)   selecting a second encryption algorithm from [[the]] a group consisting of: (i) no encryption, and (ii) those encryption algorithms requiring less processing overhead than required by said first encryption algorithm;

(d)   producing from a second part of said message a second data set incorporating encryption to an extent determined by said step of selecting a second encryption algorithm; and

(e)   generating signals that transmit to a receiving device, over at least one transmission channel, said first and second data sets and information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively; and

(f)   providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message.

32.   (Currently Amended) The method of claim 31, including the further step of further comprising:

determining at said receiving device whether at least part of said first data set should be decrypted upon receipt, and if so decrypting at least part of said first data set to produce data from said first part of said message.

Atty. Dkt. No. 1875.3820001

33.   (Currently Amended) The method of claim 31, ~~including the further step of~~ further comprising:

determining whether at least part of said second data set should be decrypted upon receipt, and if so decrypting at least part of said second data set to produce data from said second part of said message.

34.   (Currently Amended) The method of claim 31, wherein said information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively comprises header information identifying those portions of the transmitted signal to which the first and second encryption algorithms were applied.

35.   (Currently Amended) The method of claim 31, wherein step (e) further ~~includes the step of~~ comprises:

transmitting to the receiving device information defining at least one of the first and second encryption algorithms.

36.   (Currently Amended) The method of claim 31, wherein in step (e) said first and second data sets are divided into packets and a plurality of said packets are transmitted in frames incorporating said information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively.

37.   (Currently Amended) The method of claim 36, wherein at least one said frame is transmitted with a flag bit to indicate a level of encryption of the data.

38.   (Currently Amended) A system for securely transmitting a message to a receiving device, comprising:

(a) first processing means for encrypting a first part of said message with a first level of encryption to produce a first message portion;

(b) second processing means for encrypting a second part of said message to produce a second message portion, using a second level of encryption from [[the]] a group consisting of: (i) no encryption, and (ii) a level of encryption less strong than said first level of encryption;

(c) transmitting means operably connected to said first processing means and said second processing means for transmitting said first and second message portions over at least one transmission channel; and

[[(e)]] (d) output means connected to receive information from said transmission channel for providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message.

39.   (Currently Amended) The system of claim 38, further comprising:

means for determining whether at least part of said first message portion should be decrypted upon receipt, and if so decrypting at least part of said first message portion to produce data from said first part of said message.

40.   (Currently Amended) The system of claim 39, further comprising:

means for determining whether at least part of said second message portion should be decrypted upon receipt, and if so decrypting at least part of said second message portion to produce data from said second part of said message.

41.   (Currently Amended) The system of claim 38, wherein said first processing means encrypts said first part of said message with an asymmetric algorithm and said output means further includes means for decrypting said first message portion on receipt for use by the receiving device.

42.   (Currently Amended) The system of claim 38, wherein said first processing means encrypts said first part of said message for transmission, said second processing means uses no encryption for said second part of said message, and said output means provides said first message portion to the receiving device without

decrypting said first message portion, whereby said receiving device can process said second part of said message but cannot interpret said first part of said message.

43.   (Currently Amended)   The system of claim 38, wherein said first processing means encrypts said first part of said message for transmission, said second processing means encrypts said second part of said message with said second level of encryption less strong than said first level of encryption, and said output means comprises means for decrypting said second message portion upon receipt.

44.   (Currently Amended) The system of claim 43, wherein said output means further comprises means for decrypting said first message portion upon receipt.

45.   (Currently Amended)   The system of claim 38, wherein said first processing means encrypts said first part of said message, said second processing means applies no encryption to said second part of said message, and said output means includes means for decrypting a first subset of said first message portion and providing to said receiving device said decrypted first subset of said first message and a second subset of said first message that is not decrypted.

46.   (Currently Amended)   The system of claim 38, wherein said first processing means encrypts said first part of said message, said second processing means encrypts said second part of said message with said second level of encryption less strong than said first level, and said output means includes means for decrypting a first subset of said first message portion and providing to said receiving device said decrypted first subset of said first message and a second subset of said first message that is not decrypted.

47.   (Currently Amended) The system of claim 46, wherein said output means comprises means for decrypting said second message portion upon receipt and providing a resulting decrypted second message portion to the receiving device.

48.   (Currently Amended) The system of claim 38, wherein said transmission means comprises means for dividing said first message portion and said second message portion into frames alternately transmitting frames of said first and second message portions over said at least one transmission channel.

49.   (Currently Amended) The system of claim 38, wherein said message comprises speech data and said transmission channel comprises a mobile telephone system channel.

50.   (Currently Amended) The system of claim 49, wherein a fraction of the speech data sufficient to prevent understanding of an intercepted message is encrypted and transmitted in said first message portion.

51.   (Currently Amended) The system of claim 49, wherein said message includes video telephone data and said video telephone data is at least partially encrypted and decrypted upon receipt only if one or more subscribers involved in the message exchange is a video telephone service subscriber.

52.   The system of claim 49, further comprising:

means for encoding said speech data to produce a coded data set;

means in said first processing means for encrypting and transmitting in said first message portion encoding data useful in decoding said coded data set;

means in said second processing means for selecting and applying said second level of encryption to said coded data set to form said second message portion;

means in said output means for decrypting said encoding data upon receipt;

whereby said receiving device receives and uses said encoding data to decode said coded data set to obtain said speech data.

53.   (Currently Amended) The system of claim 52, wherein said means for encoding said speech data incorporates a speech codec.

Atty. Dkt. No. 1875.3820001

54.   (Currently Amended) The system of claim 38, wherein said transmission means includes means for transmitting information indicating which portions of the transmission are encrypted.

55.   (Currently Amended) The system of claim 54, wherein said transmission means includes framing means for separating said first message portion and said second message portion into a plurality of frames.

56.   (Currently Amended) The system of claim 55, wherein said framing means includes means for adding to said encrypted frames an indication of an applied level of encryption.

57.   (Currently Amended) The system of claim 56, wherein said indication is a frame encryption flag.

58.   (Currently Amended) The system of claim 38, wherein said message comprises video data and said transmission channel comprises a video distribution channel.

59.   (Currently Amended) The system of claim 58, wherein said video distribution channel comprises a cable television distribution channel.

60.   (Currently Amended) The system of claim 58, further comprising:

means for selecting a plurality of key data elements of said video data containing information needed to properly process and display the video data;

means associated with said first processing means for encrypting and transmitting in said first message portion said key data elements;

means associated with said second processing means for selecting and applying said second level of encryption to at least some of said video data not designated as key data elements;

decryption means associated with the output means for decrypting said key data elements upon receipt;

whereby said receiving device is provided with said data from said key data elements and uses said key data to process and display said video data.

61.   (Currently Amended)   The system of claim 60, wherein said key data elements contain I-signal video information.

62. - 67. (Cancelled)

68.   (Currently Amended)   A system for securely transmitting a message to a receiving device using a first encryption algorithm and a second encryption algorithm selected selectable from [[the]] a group consisting of: (i) no encryption, and (ii) those algorithms requiring less processing overhead than required by said first encryption algorithm, comprising:

(a) first processing means for encrypting a first part of said message with said first encryption algorithm to produce a first data set;

(b) second processing means for producing from a second part of said message a second data set incorporating encryption to an extent determined by said second encryption algorithm;

(c) transmission means for generating signals for transmission to a receiving device over at least one transmission channel, said signals representing said first and second data sets and information sufficient for said receiving device to determine a type of encryption applied to at least one of said first and second data sets respectively; and

(d) output means for providing an output at the receiving device including at least one of: at least part of said data from said first part of said message and at least part of said data from said second part of said message.

69.   (Currently Amended)   The system of claim 68, wherein the output means further includes means for decrypting at least part of said first data set to produce data from said first part of said message.

70. (Currently Amended) The system of claim 69, wherein the output means further includes means for decrypting at least part of said second data set to produce data from said second part of said message.

71. (Currently Amended) The system of claim 68, wherein said transmission means further comprises means for generating and transmitting header information identifying those portions of the transmitted signal to which the first and second encryption algorithms were applied.

72. (Currently Amended) The system of claim 68, wherein said transmission means further comprises means for transmitting to the receiving device information identifying at least one of the first and second encryption algorithms.

73. (Currently Amended) The system of claim 68, wherein said transmission means further comprises framing means for dividing said first and second data sets into packets and transmitting said packets in frames incorporating said information sufficient for said receiving device to determine the type of encryption applied to at least one of said first and second data sets respectively.

74. (Currently Amended) The system of claim 73, wherein at least one said frame is transmitted with a flag bit to indicate a level of encryption of the data.

Atty. Dkt. No. 1875.3820001